FAA National Software Conference
Avionics Computer Resource

AVIONICS COMPUTER RESOURCE (ACR)

Bob Patterson
Chairman RTCA SC-182

Rockwell Collins

WHAT IS AN ACR?

- A General Purpose Computing Platform Optimized for Avionics Applications
  - Defined Application / Programming Interface
  - Partitioning / Protection
  - Health Monitoring
- Includes "Device Drivers" and Physical Layer Interface With Aircraft
- Analogous to:
  - Pentium + Windows or
  - Power PC + MAC os

Rockwell Collins

FAA National Software Conference
Avionics Computer Resource

WHO WANTS AN ACR?

- Air Transport Operators
  - Extension of AEEC Integrated Modular Avionics
- General Aviation
  - Interest from AGATE

Rockwell Collins

WHAT BENEFIT DOES IT OFFER?

- Opportunity to Normalize Function and Operation Across a Fleet of Multiple Aircraft Types
- Flexibility for Frequent Configuration Changes
- Reduction in Certification Effort of Re-Used Components
- Shorter Development Cycle Time
- Economy of Scale for Software Developer
- Economy of Scale for Hardware Developer

Rockwell Collins

MORE BENEFITS

- Open System Concept
  - Independent Development of Platform and Application Programs
- Draws Technology from Computer Industry
- Appliance Approval Independent of Aircraft Installation

Rockwell Collins

RTCA SC-182 CHARTER / STATUS

- Requested by Air Transport Operators
- Task: Prepare MOPS for an ACR
- 8/99: Completed Draft MOPS
- EUROCAE Changed Title to, "Requirements Specification for ACR"
- 2/00: ED-96 Adopted
- 6/00: DO-255 Adopted

Rockwell Collins

SC-182 CHALLENGE

- Specify ACR Characteristics Sufficient for a Certification Basis
- Remain Flexible to Accommodate Computer Technology Advances

Rockwell Collins

SC-182 COMPROMISE

- The Requirements Specification for ACR Is a "Specification for a Specification"
  - Specific Attributes & Services Are Mandated
  - Extensions, Interrupts and Fault Tolerance Are Allowed
- API, Performance & Capacity Are Declared By the ACR Supplier
  - A Data Sheet Is Mandated
  - Assurance of Data Sheet Information Is Mandated
  - DO-160 and DO-178 Compliance is Mandated

Rockwell Collins

SECTION 1

- Introduction
  - Draws Attention to the Unusual Nature of the Document (As Opposed to a Traditional MOPS)
  - Distinguishes Between the Platform and Application Software
  - Acknowledges That Each Integration of Platform and Application Software Must be Evaluated In the Context of an Aircraft Certification

Rockwell Collins

SECTION 2

- Requirements and Qualification
  - Stipulates:
    - Data Sheet Required
    - Mandatory Attributes and API Services
    - Declaration of Performance and Capacity
    - Assurance of Data Sheet Values Required
  - Allows:
    - Extended API Services
    - Interrupts
    - Fault Tolerance

Rockwell Collins

SECTION 2

- Mandated Attributes
  - Defined API
  - Deterministic Resource Allocation
  - Isolation Between Applications and Core S/W
  - Isolation Between Applications
  - Compliance With DO-178B
    - Level Must be Declared

Rockwell Collins

SECTION 2

- Mandated API Services
  - Partition Management
  - Process Management
  - Time Management
  - Memory Management
  - Communication
  - Health Monitoring
  - Field Loadable
- Data Sheet Expectations are Given for Each Service

Rockwell Collins

SECTION 2

- Allowable Capability
  - Extended API Services
  - Interrupts
  - Fault Tolerance
- Data Sheet Expectations are Given for Extended Services

Rockwell Collins

SECTION 2

- Performance (& Capacity) Parameters
  - CPU Type, Instruction Set, Cache
  - Partitions; Number, Duration, Jitter
  - Context Switch Time
  - Memory; Allocation, Addressing, Access Time
  - Communication; Type, Quantity, Capacity, Rate, Delay
  - I/O; Type, Quantity, Queuing, Propagation Delay
  - Power On / Interrupt Characteristics
- Data Sheet Expectations are Given for each Parameter

Rockwell Collins

SECTION 2

- Environmental Qualification
  - Compliance With DO-160D Is Required
  - Categories Must be Declared
  - Testing Must Assure Acceptable Operation and Performance of System Services, I/O Interfaces, Partition Integrity and Allocation of Resources to Partitions.

Rockwell Collins

SECTION 2

- Function and Operational Assurance
  - Objectives Established for Each Service and Performance Parameter
  - Test and / or Analysis Allowed

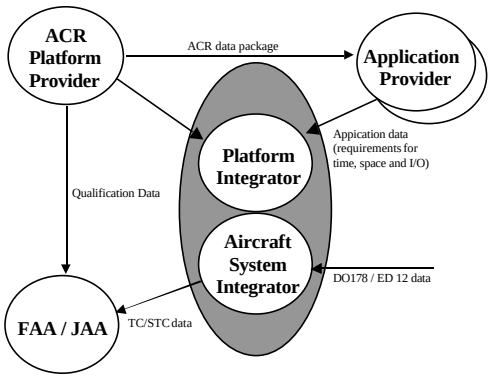
Rockwell Collins

SECTION 3

- Integration, Installation and Certification
  - Highlights Relationships Between Platform Provider, Application Provider(s), Integrator and Regulatory Authority
  - Requires Consideration of ACR Performance With the Mix of Applications Hosted
  - Requires System Level Safety Assessment
  - Requires Analysis of Resource Quantity, Allocation, and Contention

Rockwell Collins

RELATIONSHIPS



Rockwell Collins

SECTION 4

- Certification of Modified Systems
  - Gives Credit for "Qualification" of ACR Platform Attributes
  - Suggests That Previously Approved Data be Re-Used Where Unchanged

Rockwell Collins

ANNEX A

- Data Sheet for ACR Attributes
  - Tracks Requirement Paragraphs In Section 2
  - Leads the ACR Supplier to Describe the Implementation
  - Leads the ACR Supplier to Site Assurance

Rockwell Collins

DATA SHEET SAMPLE

Table A-1: ACR data sheet template "Function and Operation" (continued)

Group	ID	Attribute	Implementation	Means of Verification
Process Management Section 2.1.1.2 / 2.5.1.2	SRV3.1	Obtain the ID of the current process	*GET_PROCESS_ID*	
	SRV3.2	Obtain the status of the current process	*GET_PROCESS_STATUS*	
	SRV3.3	Define a new process	*CREATE_PROCESS*	
	SRV3.4	Set the priority of the current process.	*SET_PRIORITY*	
	SRV3.5	Suspend a process	*SUSPEND_SELF* *SUSPEND*	
	SRV3.6	Reactivate a suspended process	*RESUME*	
	SRV3.7	Stop/halt a process	*STOP_SELF* *STOP*	
	SRV3.8	Activate a process	*START*	
	SRV3.9	Prevent the current process from being pre-empted (turn preemption off)	*LOCK_PREEMPTION*	
	SRV3.10	Preemption on	*UNLOCK_PREEMPTION*	

Rockwell Collins

ANNEX B

- **Application Interface Specification Example**
  - **Drawn From ARINC Specification 653**
  - **Modified to Support SC-182 Notion of API**
  - **Intended to Indicate the Depth of Specification Expected in the ACR Data Sheet**

Rockwell Collins

ANNEX C & D

- Glossary of Terms
- List of Acronyms

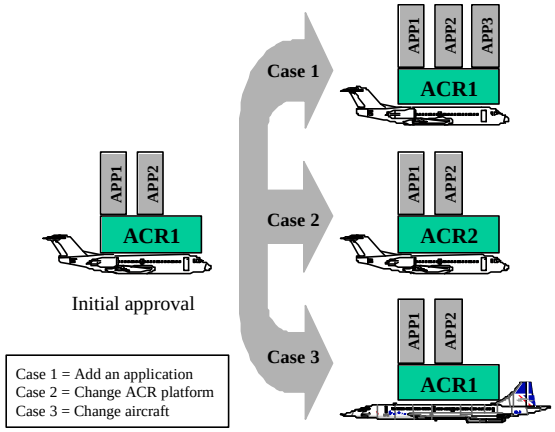
Rockwell Collins

ANNEX E

- Re-Use Benefits
  - Illustrates 3 Follow-on Certification Scenarios
    - Addition of New Application
    - "Port" Application Set to Another ACR
    - Install ACR & Applications in Another Aircraft Model
  - Examines DO-178B Objectives
  - Suggests Where Life Cycle Data May Be Re-Usable

Rockwell Collins

3 SCENARIOS



Case 1 = Add an application
Case 2 = Change ACR platform
Case 3 = Change aircraft

Rockwell Collins

RE-USE SAMPLE

Table E-1: Verification of Verification Process Results (COMMENTARY)

(reference to DO-178B / ED-12B, table A-7)

	Objectives		Applicability By SW Level				Degree of reuse / comments		
	Description	Ref.	A	B	C	D	Case 1 Add an application	Case 2 Change ACR platform	Case 3 Change aircraft
1	Test procedures are correct.	6.3.6b	●	❍	❍		R	PR The test set-up may have to change	R
2	Test results are correct and discrepancies explained.	6.3.6c	●	❍	❍		R	NR	R
3	Test coverage of high-level requirements is achieved	6.4.4.1	●	❍	❍	❍	R	NR	R
4	Test coverage of low-level requirements is achieved	6.4.4.1	●	❍	❍		R	NR	R
5	Test coverage of software structure (modified condition/decision) is achieved.	6.4.4.2	●				R	NR	R
6	Test coverage of software structure (decision coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●			R	NR	R
7	Test coverage of software structure (statement coverage) is achieved.	6.4.4.2a 6.4.4.2b	●	●	❍		R	NR	R
8	Test coverage of software structure (data coupling and control coupling) is achieved.	6.4.4.2c	●	●	❍		R	NR	R

R = Reusable: Life cycle data from initial approval is unchanged and reusable for follow-on certification
PR = Partially Reusable: Changes to life cycle data from initial approval must be evaluated during follow-on certification
NR = Not Reusable: Life cycle data from initial approval is not applicable for follow-on certification

Rockwell Collins